REMARKS

This Amendment is filed in response to the aforementioned non-final Office Action (hereafter "Office Action") in relation to the Reissue Application for U.S. Patent No. 5,848,159 (hereafter the "original patent"). All changes presented herein have been made vis-à-vis the original patent to be issued.

I. Reexamination Proceedings and Reissue Application Merged

Merger of the Reexamination proceedings 90/005,733 and 90/005,776, with respect to the original patent and the Reissue Application 09/694,416 (for the reissue of the original patent) is hereby acknowledged (See: Section 1 in the Detailed Action of the Office Action). In keeping with the procedures set forth for handling the merged proceedings, and to maintain prosecution and examination consistency between the Reissue and Reexamination proceedings, Applicants will submit a separate Housekeeping Amendment in each of the Reexamination proceedings.

II. Status of the Claims

As of the date of this Amendment, claim 8 of the original patent is canceled, claims 1-7 and 9-13 of the original patent are amended and remain pending; new claims 14-61 were added in the preliminary amendment and, of these claims, claims 14-40, 42, 43, 45-47, 50-56 and 58-61 are hereby amended. Thus, claims 1-7 and 9-61 are now pending in the Reissue Application.

III. Claim Designated for Printing in the Official Gazette

Claim 1 is designated for printing in the Official Gazette upon allowance of this Reissue Application.

IV. Statement of Support for the Amendments in the Disclosure of the Original Patent

A. All changes made vis-à-vis the original patent

All the amendments presented herein, including amendments to the written description and the claims, have been made vis-à-vis the original patent. Accordingly, the amendments presented herein include the amendments previously presented in the Preliminary Amendment,

which was filed concurrently with this Reissue Application, to the extent that such amendments are to be maintained. Moreover, the statements of support for the amendments herein, even if some have already been stated before in the Preliminary Amendment and repeated herein, are provided in their entirety for completeness and clarity.

B. The Specification

The specification of the original patent has been amended to correct typographical errors and other matters of form and to render the specification consistent throughout and with the claims. Support for the amendments to the specification may be found throughout the original patent. No new matter has been introduced by the amendments to the specification.

In general, changes embodying corrections of typographical errors and other matters of form are self-explanatory and need no further explanation. As to the mathematical expressions, equations expressing any congruence of the form $b=c(\text{mod } m)$ or the like, where b is congruent to c and m is the modulus, are mathematically written in proper form as $b \equiv c(\text{mod } m)$. Accordingly all the equations are written in proper form, e.g., $C \equiv M^e(\text{mod } n)$. Were applicable, the parentheses (e.g., around "mod n") are properly added as well.

Support for amendments to the paragraph beginning at column (hereafter "col."), line 4 may be found in col. 1 of the cover page. Support for the amendments to the paragraph beginning at col. 3, line 23 and the paragraph beginning at col. 3, line 27 may be found for example at col. 2 of the cover page and col. 13, lines 44-47.

Support for amendments to the paragraph beginning at col. 3, line 36, may be found at column 5, lines 31-33. Support for amendments to the paragraph beginning at col. 3, line 56, may be found for example at col. 3, lines 20-26, col. 3, lines 44-55 and col. 4, lines 9-11. Support for amendments to the paragraph beginning at col. 4, line 6, may be found for example at col. 3,lines 20-26, col. 4, lines 6-12, 32-34 and 52-56.

Support for amendments to the paragraph beginning at col. 4, line 13 and the paragraph beginning at col. 4, line 50, may be found for example at col. 3 line 42, col. 4, line 41, and col. 10, lines 54-56. Further support for amendments to the paragraph beginning at col. 4, line 50 may be found at col. 4, lines 50-52.

Support for paragraph inserted before the paragraph beginning at col. 5, line 52, may be found for example at col. 14, lines 30-36 and 45-49. Support for amendments to the paragraph beginning at col. 5, line 30, may be found for example at col. 2, lines 5-10, col. 3, line 42, col. 4 line 41, col. 5, line 39, col. 10, line 65 and col. 11, lines 8-9. Further support for amendments to the paragraph beginning at col. 5, line 30, may be found in the multitude of mathematical expressions where d, the private key portion, is the "exponent," e.g., $M \equiv C^d \pmod{n}$ at col. 6, lines 1-5.

Support for amendments to the paragraph beginning at col. 6, line 24, may be found for example at col. 5, lines 31-33, col. 6, line 37 ("$M=Y_k\ldots$"), col. 7, line 15, and col. 11, lines 15-20. Support for amendments to the paragraph beginning at col. 6, line 65, may be found for example at col. 6, lines 1-4, 26-35, 40-53 and 67. Support for amendments to the paragraph beginning at col. 7, line 1, may be found for example at col. 2, lines 32-34 and 40, col. 3, lines 22-26, col. 4, lines 32-34, col. 6 line 38 and col. 7, lines 56-58.

Support for amendments to the paragraph beginning at col. 8, line 1, is fund in col. 8 line 3 (i.e., FIPS 140-1 with level 3 is a well known standard, See: http://csrc.nist.gov/fips/fips1401.htm). Support for amendments to the paragraph beginning at col. 10, line 15, may be found for example at Figure 3. Support for amendments to the paragraph beginning at col. 10, line 35, may be found for example in col. 10 line 40 and line 53 (i.e., M is represented by a numerical value greater than *0* and smaller than *n*).

C. The Claims

Claims 1-7 and 9-13 of the original patent have been amended to correct typographical errors and other matters of form, to explicitly recite subject matter which is implicitly included in the claimed invention, and/or to more clearly and particularly recite the subject matter which Applicants regard as their invention. New claims 14-61 have been added to further point out and distinctly claim the subject matter that Applicants regard as their invention.

For the Examiner's convenience, a clean version of the amended claims (as now presented) is provided herewith as **Exhibit A**. As stated above, the amendments herein are made vis-à-vis the original patent (notwithstanding the prior changes to the claims in the Preliminary Amendment). But to show the difference between the claims presented in the Preliminary

Amendment and the claims presented herein a mark-up version showing the changes relative to the Preliminary Amendment is provided as **Exhibit B**.

Support for the amendments to claims 1-7 and 9-13 and for the added claims, 14-61, may be found throughout the original patent. No new matter has been introduced by this amendment.

In general, claim amendments embodying corrections of typographical errors, antecedent basis errors, and other matters of form are self-explanatory and need no further explanation. As to the mathematical expressions, equations expressing any congruence of the form $b=c(\text{mod } m)$ or the like, where b is congruent to c and m is the modulus, are mathematically written in proper form as $b\equiv c(\text{mod } m)$. Accordingly all the equations are written in proper form, e.g., $C\equiv M^e(\text{mod } n)$. Were applicable, parentheses (e.g., around "mod n") are properly added as well.

Also, by and large, claim amendments representing a change to the preamble of the original and new (added) independent claims find support throughout Applicants' original patent. Particularly, support for the recitation of *communications of a message cryptographically processed with RSA (Rivest, Shamir & Adleman) public key encryption*, is implicitly present in the mathematical expressions throughout Applicants' original patent. Additionally, support for this recitation is explicitly present in the summary at col. 3 and col. 4, in the detailed description at col. 5 et seq. as well as in the Rivest patent (4,405,829) which is incorporated by reference into the original patent (See, e.g., col. 1, lines 56-63). Accordingly, this particular amendment will not be addressed again with respect to each individual claim.

Support for the amendments to claim 1 as now presented may be found, for example, at claims 1, 5 & 6 as presented in the original patent as well as at col. 1, lines 32-42 & 43-54, col. 3, lines 7-12, 22-25 & 39-44, col. 4, lines 6-8 & 32-48, col. 5, lines 30-36, 40-46 & 58-63, and col. 10, lines 25-34. Support for the amendments to claim 2 as now presented may be found, for example, at the original claims 2 & 4 as well as at col. 5, lines 36-50. Similarly, support for amendments to claims 3-7 and 9-13 as now presented may be found, for example, at claims 1-7 and 9-13 as presented in the original patent. Further support for the amendments to claims 3-7 and 9-13 as now presented may be found for example at col. 1, lines 32-42 & 43-54, col. 3, lines 39-44, col. 5, lines 30-50, col. 7, line 44 to col. 10, line44. Further support for amendments to claims 9-13 as now presented may be found for example at col. 9, lines 16-23 & 47-58.

As to the newly added claims, support for claim 14-23 and 40-59 may be found, for example, at col. 1, lines 32-45, col. 3, lines 30-50, col. 4, lines 32-49, col. 5, lines 30-51, col. 5,

line 66 to col. 6, line 25, col. 7, line 44 to col. 10, lines 44. Further support for new claims 14-23 and 40-59 may be found at claims 1-13 as presented in the original patent. For example, support for new claims 18 and 19 may be found in claim 9, i.e., col. 14, lines 30-36. Also, support for new claims 24-39 may be found for example at column 3, lines 36-65, col. 4, lines 8-12, 32-38 & 50-56 and col. 5, lines 58-63. Support for new claims 42-52 may be found at Figures 1-3, and the accompanying description at col. 7, line 34 to col. 10, lines 44. Further support for new claims 50-54 may be found at col. 5, line 52 to col. 6, line 6. Finally, support for claims 60 and 61 may be found at col. 4, lines 6-13 and col. 5, lines 61-63.

V. Supplemental Reissue Oath and Declaration

Applicants appreciate the reminder about a Supplemental Reissue Oath and Declaration (See: Section 3 in the Detailed Action of the Office Action, or simply Section 3 of the Office Action). Applicants will submit that Oath and Declaration document at the close of prosecution, after allowance of this Reissue Application.

VI. Consent by Assignee, Certificate Establishing Rights of Assignee, and Assignments

In reference to Sections 4 & 5 of the Office Action, where it is stated that the Reissue Application is objected to as lacking written consent of all assignees, including Tandem Computers Inc. ("Tandem") and Compaq Computer Corp. ("Compaq"), Applicants point out that the requirements under 37 CFR §§1.172 & 3.73 have been met. For the Examiner's convenience **Exhibit C** includes a copy of documents which show compliance with these requirements, including: Consent of Assignee to this Reissue Application, Certificate under 37 CFR 3.73(b), Notice of Recordation of the Assignment from the inventors to Tandem and Notice of Recordation of Merger Documents relating to the merger of Tandem into Compaq. A copy of the stamped return postcard showing filing the said documents is also provided.

To recap, the inventors (Collins et al.) assigned their invention (U.S. Application No. 08/784,453) to Tandem, which Assignment has been recorded on May 7, 1997 at Reel/Frame 8542/0875. In turn, Tandem assigned its Patent Applications and issued Patents to Compaq when Tandem merged into Compaq. To that end, the Merger Documents have been filed with the Assignment Division in relation to the aforementioned U.S. Patent 5,848,159 (which issued from the 08/784,453 Application to Collins at al. on December 8, 1998, and the reissue of which is

now being sought). As the enclosed Notice of Recordation of the Merger Documents indicates, the Merger Documents have been recorded on October 16, 2000 at Reel/Frame 011190/0457.

Accordingly, all the requirements under 37 CFR §§1.172 & 3.73 have been met. Respectfully, in view of the foregoing the objection to this Reissue Application should be reconsidered and withdrawn.

VII. The Drawings

In reference to Section 6 of the Office Action, where it is stated that new formal drawings are required, Applicants hereby comply. Attached herewith are new formal drawings, including Figures 1-3.

VIII. Preliminary Amendment Entered

In Section 7 of the Office Action it is indicated that the Preliminary Amendment, filed concurrently with this Reissue Application, has been entered. Applicants appreciate entry of the Preliminary Amendment and note that, notwithstanding, this amendment introduces changes vis-à-vis the original patent as required by 37 CFR §1.173(g).

IX. Three Information Disclosure Statements Considered

In Section 8, the Examiner states that the information disclosure statements (IDSs) filed April 11, 2001 (4 references) and June 26, 2001 (2 references), respectively, where considered (on December 5, 2001 & June 4, 2002, respectively). On December 5, 2001, The Examiner considered also, but failed to mention, the IDS (13 references) filed concurrently with this Reissue Application. A copy of all three IDS was signed by the Examiner and returned with this Office Action. A copy of the three, signed IDSs is provided for the Examiner's convenience as **Exhibit D**.

X. Objection to the Specification

A. New Matter

Section 10 of the Office Action indicates that the [preliminary] amendment to the specification has been object to under 35 U.S.C. §132 having allegedly introduced new matter to the specification. In particular, the objection to the added material at col. 5, line [62] relating to

'digital signatures' alleges that digital signatures have not been disclosed in the originally-filed specification (implicitly or explicitly).

However, the Examiner is kindly requested to note the recitations in claims 9 and 10 of the original patent. Likewise, it is implicit in RSA schemes, as disclosed in the original specification (e.g., col. 1, lines 55-62), that $C \equiv M^d \pmod{n}$ [or $M_s \equiv M^d \pmod{n}$] produces a value typically referred to as the "signature" (as the private key d is used in the encryption). Indeed, in col. 10, lines 35-37 & 42-44 it is suggested that a plaintext message can be encrypted/decrypted using the public/private key RSA scheme. Moreover, since the original patent incorporates by reference U.S. Patent 4,405,829 (See: Col. 1, line 61), the Examiner is kindly requested to also note, in the '829 patent, col. 3, line 9 et seq. col. 5, lines 45-47, and col. 8 line 56-67.

Namely, the aforementioned amendment to Col. 5 relating to the signature merely expresses that which is implicit and/or imports that which is incorporated by reference. Accordingly, its is respectfully submitted that no new matter has been introduced by the aforementioned amendment to Col. 5 relating to the signature. A reconsideration and withdrawal of the new matter objection under 35 U.S.C. §132 is hereby solicited.

B. Informalities

As indicated in Sections 11-13 of the Office Action, the specification is objected to because of the error in equation 4 in the paragraph starting at col. 2 line 19, and because of a misstatement of line number [52] at col. 8. Applicants appreciate the Examiner's thorough review of the original patent and Preliminary Amendment and have corrected these deficiencies. As now presented equation 4 correctly recites:

$$\underline{M \equiv C^d \pmod{n}} \qquad (4),$$

and the line number of the paragraph at col. 8 is changed to 62. The specification is now believed to be correct, and reconsideration and withdrawal of the objection to the specification based on informalities is hereby respectfully solicited.

XI. Claim Objections

In Sections 14-17, the Examiner points out deficiencies in amendments to claim 3 as presented in the preliminary amendment. Claim 3 has been amended in accordance with the

mark-up version of the claims as shown herein above and is now believed to be correct (See, e.g., $M_x" \leq n_y-1$, and $C_x \equiv M_x"^{e_y} (\mathrm{mod}\, n_y)$). Accordingly, reconsideration and withdrawal of the claim objections is respectfully requested.

XII. Claim Rejections under 35 U.S.C. §101; Rejections Rendered Moot by Amendments

Sections 18-21 of the Office Action indicate that claims 7, 8 and 13 are rejected under 35 U.S.C. §101 as lacking utility (See: Sections 18-21 of the Office Action). Although the comments immediately below address these claim rejections, as later explained, the rejections have nonetheless been rendered moot by the claim amendments as presented herein above.

With reference to these rejections, the Examiner asserts that an invention that is useful for encryption *only* fails to provide utility and is of no use if it cannot be decrypted. Applicants respectfully disagree with the Examiner's characterization of the claimed invention (as recited in the earlier claim 7) and in view of that disagree that the claimed invention lacks utility. Indeed, as previously presented claim 7 did *not* provide *only* for *encoding* and did not preclude decoding (and claim 8 (now cancelled) explicitly recited a decoding key D_i for each terminal).

The Examiner also notes that the invention is directed, in general, to increasing the efficiency of an RSA cryptographic system and method. And, it is true that increasing the speed of encryption (by reducing the number of computation cycles) is useful, as the Examiner points out. Moreover, claim 7 as previously presented recited a method for 'establishing cryptographic communications' and encryption establishes cryptographic communications. Namely, the invention as recited in the earlier claim 7 produced the specifically useful result claimed by Applicants. Hence, earlier claims 7 and 8 did not lack utility.

Notwithstanding the foregoing, the claim rejections have been rendered moot by the claim amendments herein above. As will be later discussed in more detail, the claims have been amended (as shown herein above) to explicitly claim "communications of messages cryptographically processed with RSA public key encryption" (as is well known, RSA stands for Rivest, Shamir and Adleman). To be sure, a message can contain, for example, a DES key (data encryption standard key). Then, in accordance with this invention each messages, even if containing a DES key, is cryptographically processed using the RSA scheme.

It is respectfully submitted that all the claims produce the results claimed by Applicants and hence have utility. Accordingly, the claim rejections under 35 U.S.C. §101 should be reconsidered and withdrawn.

XIII. Claim Rejections under 35 U.S.C §112

A. Enablement, 35 U.S.C. 112, 1st paragraph

Claims 8 and 13 are rejected under 35 U.S.C. 112, 1st paragraph, for lack of enablement (See: Sections 23-25 of the Office Action). Claim 8 has been cancelled without prejudice or surrender of subject matter and will not be discussed here. Claim 13, however, remains pending and is enabled by Applicants' disclosure including the disclosure that Applicants incorporated by reference into the written description. Claim 13 is enabled, for example, by the description in the original patent at col. 1, lines 54-55 and col. 7, lines 25-33, and in the 4,405,829 patent at col. 13, lines 29-46. Accordingly, reconsideration and withdrawal of the claim rejection under 35 U.S.C. 112, 1st paragraph is hereby respectfully requested.

B. Distinctly Claiming Applicants' Invention, 35 U.S.C. 112, 2nd paragraph

In Sections 26-30 of the Office Action the Examiner indicates that claims 24-39 are rejected under 35 U.S.C. 112, 2nd paragraph. However, the claim amendments obviate these claim rejections as the terms "faster than..." and "compatible with..." are not recited and the term "fewer computation cycles..." for multi-prime RSA is recited comparatively to the cycles for two-prime RSA. Applicants believe that given the above-outlined amendments to claims 24-39 Applicants' invention is particularly pointed out and distinctly claimed. Moreover, as mentioned in Section IV.C above, support for these claims is found in Applicants' disclosure. Accordingly, reconsideration of the claim rejections under 35 U.S.C. 112, 2nd paragraph is hereby respectfully requested.

XIV. THE INVENTION

Before getting to the claim rejections in the next section (XV) an explanation of the invention is worthwhile. It is important that the invention be properly understood particularly in view of the assertions and analysis in the Office Action.

First, even though it is clear from the mathematical expressions throughout Applicants' disclosure, including the claims, that the invention involves RSA public key encryption, the claims have been amended to expressly point this out. As now presented, the claims make it expressly clear that they involve messages that are cryptographically processed with RSA public key encryption. Having said that, important aspects of the claimed invention are further explored.

Note for example claim 1. The clean version of claim 1 as now presented reads as follows:

1. (Twice Amended) A method for communications of a message cryptographically processed with RSA (Rivest, Shamir & Adleman) public key encryption, comprising the steps of:
developing k distinct random prime numbers p_1, p_2, . . . p_k, where k is an integer greater than 2;
providing a number e relatively prime to $(p_1 -1)\cdot(p_2 -1)\cdot\ldots\cdot(p_k-1)$;
providing a composite number n equaling the product $p_1\cdot p_2\cdot . . . .\cdot p_k$;
receiving a ciphertext word signal C which is formed by encoding a plaintext message word signal M to a ciphertext word signal C, where M corresponds to a number representative of the message and $0\leq M \leq n-1$,
where C is a number representative of an encoded form of the plaintext message word signal M such that
$C\equiv M^e \pmod n$, and where e is associated with an intended recipient of the ciphertext word signal C; and
deciphering the received ciphertext word signal C at the intended recipient having available to it the k distinct random prime numbers p_1, p_2, . . . p_k.

In essence, claim 1 recites a method in which a message M is cryptographically processed (encoded) using the public key of a recipient (e,n). The encoded message $C\equiv M^e \pmod n$, known as ciphertext, is received in that form without further modification by the recipient. That same (received) ciphertext C, is indeed decipherable by the recipient (using its private key (d,n)). As is next explained, the recipient has available to it the k factors from which the modulus n is produced.

The recitation in claim 1 includes developing k distinct random prime numbers $p_1, p_2, \ldots p_k$, where k is an integer greater than 2 and further includes the fact that the modulus n is a composite number equaling the product $p_1\cdot p_2\cdot . . . .\cdot p_k$. Namely, claim 1 recites that $k>2$ and the k prime numbers are random and distinct. Moreover, claim 1 recites that the modulus n is provided from a product of the k prime numbers. Contrast this (claim 1) recitation with selecting a modulus n **and then** factoring n to the k prime numbers.

It is important to understand and keep in mind that providing n as the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ having [already] available the k prime numbers makes it possible for them to be random and distinct. The randomness and distinctness attributes of the k prime numbers will materially improve the security in any cryptographic system with RSA public key encryption.

Moreover, the use of $k>2$ prime numbers allows improved efficiency of such system. As one would imagine, developing three or more prime numbers each of smaller size (relative to each of a pair of primes for the same size n) takes fewer computation cycles than it would take for developing the pair of (larger) prime numbers. As an additional time-saving benefit, the k prime numbers allow parallel processing of encryption tasks.

By analogy, in each of the other claims (original and added claims) n is a product of the k prime factors, where $k>2$ and where the k prime factors are random and distinct. Again, contrast this with selecting a modulus n and then factoring n to k prime numbers (even if n were randomly selected). In addition, claims, including claims 2-6, 9, 11, 15, 16 etc., indicate that d (the private key portion) is established as a function of e (the public key portion) and the k prime numbers. As recited for example in claim 2, d is a multiplicative inverse of $e(\text{mod}(\text{lcm}(p_1 - 1, p_2 - 1 \ldots p_k - 1)))$; and, again, the k ($k>2$) distinct random prime numbers $p_1, p_2, \ldots p_k$ from which the modulus n is provided/computed are used for establishing d.

Within the scope and spirit of the invention as originally disclosed one would also recognize such variations as recited for example in claim 7. A clean version of claim 7 reads as follows:

7. (Amended) A method for communications of a message cryptographically processed with an RSA public key encryption, comprising the steps of:

developing k factors of a composite number n, the k factors being distinct random prime numbers and k is an integer larger than two (k>2);

providing a number e relatively prime to a lowest common multiplier of the k factors;

providing the composite number n;

receiving a ciphertext word signal C which is formed by encoding a digital message word signal M to the ciphertext word signal C, where said digital message word signal M corresponds to a number representative ofsaid message and

$0 \leq M \leq n-1$,

where said ciphertext word signal C corresponds to a number representative of an encoded form of said message through a relationship of the form

$C \equiv a_e M^e + a_{e-1} M^{e-1} + \ldots + a_0 \pmod{n}$
where e and a_e, a_{e-1}, . . . , a_0 are numbers; and
deciphering the received chiphertext word signal C at an intended recipient with knowledge of the k factors.

In essence, claim 7 has in common with claim 1 many of the important features that make this invention so advantageous, including the modulus *n* being a product of the *k* prime factors, where *k*>2 and where the *k* prime factors are random and distinct. In addition, as is the case in claim 1, the ciphertext message (here ciphertext word signal) *C*, which is formed by encoding the message (here digital message word signal) *M*, is received without further modifications. The variation from claim 1 has to do with the manner in which the ciphertext message *C* is formed. In claim 7, the ciphertext message *C* is formed as a function of M, n, e and coeficients a_e, a_{e-1},...a_0.

Yet another variation within the scope and spirit of the disclosed invention is provided in claim 9. A clean version of claim 9 reads as follows:

9. (Twice Amended) A system for communications of message signals cryptographically processed with RSA public key encryption, comprising:
j terminals including first and second terminals, each of the j terminals being characterized by an encoding key $E_i = (e_i, n_i)$ and decoding key $D_i = (d_i, n_i)$, where i=1,2, . . . ,j, each of the j terminals being adapted to transmit a particular one of the message signals where an i^{th} message signal M_i is transmitted from an i^{th} terminal, and
$0 \leq M_i \leq n_i - 1$,
n_i being a composite number of the form
$n_i = p_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}$
where
k is an integer greater than 2,
$p_{i,1}$, $p_{i,2}$, . . . $p_{i,k}$ are distinct random prime numbers,
e_i is relatively prime to
$\text{lcm}(p_{i,1}-1, p_{i,2}-1, \ldots p_{i,k}-1)$, and
d_i is selected from the group consisting of the class of numbers equivalent
to a multiplicative inverse of
$e_i \pmod{\text{lcm}((p_{i,1}-1), (p_{i,2}-1), \ldots, (p_{i,k}-1))}$;
said first terminal including
means for encoding a digital message word signal M_1 to be transmitted from said first terminal (i=1) to said second terminal (i=2), said encoding means transforming said digital message word signal M_1 to a signed message word signal M_{1s} using a relationship of the form
$M_{1s} \equiv M_1^{d_1} (\text{mod}\, n_1)$; and

means for transmitting said signed message word signal M_{1s} from said first terminal to said second terminal, wherein said second terminal includes
means for decoding said signed message word signal M_{1s} to said digital message word signal M_1.

As in the case of claim 7, claim 9 has in common with claim 1 important features of the invention, including the modulus *n* being a product of the *k* prime factors, where *k*>2 and where the *k* prime factors are random and distinct. Additionally in common with claim 1, the ciphertext message (here signed message word signal) M_{1s}, which is formed by encoding the plaintext message (here digital message word signal) M_1, is received without further modifications. The variation from claim 1 has to do with the manner in which the ciphertext message M_{1s} is formed. In claim 9, the encoded message M_{1s} is in fact a digital signature formed as a function of M_1 and the private key of the sender (*d*,*n*).

Although additional features and variations of the invention exist, the foregoing provides a constructive explanation of the invention. In view of this explanation, one would find it easier to understand why the claimed invention, as recited in claims 1-7 and 9-61, is novel and non-obvious. The patentable differences between the claimed invention and the cited references will be further addressed below with regards to the claim rejections.

XV. Claim Rejections Under 35 U.S.C. §102

A. Summary of Claim Rejections

In Sections 31-69 of the Office Action, where it is stated that the claims (1-61) are rejected under 35 U.S.C. §102, the Examiner cites, respectivley, Rivest et al (U.S. Patent 4,405,829, hereafter "Rivest"), Vanston and Zuccheranto, "*Using four-prime RSA in which some bits are Specified*," Electronic Letters, Vol. 30, No. 35, 1994 (hereafter "Vanstone"), Captain Nemo, "*RSA Moduli should have 3 Prime Factors*," Scientific Bulgarian, August 1996, (hereafter "Nemo"), Slavin (U.S. Patent 5,974,151) and Itakura et al, "*A Public-key Cryptosystem Suitable for Digital Multisignature*," Nipon Electronic Co., Ltd., R&D No. 71, October 1983, IPSJ Journal Vol. 24, No. 4, May 2001 (hereafter "Itakura"). Rivest, Vanstone and Itakura have been relied on for rejecting the claims under 35 U.S.C. §102(b). Nemo and Slavin have been relied on for rejecting the claims under 35 U.S.C. §102(e).

1. Nemo Cannot be Relied on for Rejection under 35 U.S.C. §102(e)

Nemo is not a patent and therefore it cannot be relied on for rejecting the claims under 35 U.S.C. §102(e). As set forth in 35 U.S.C. §102(e), only a patent granted to another from an application filed prior to Applicants' date of invention can preempt allowance of this Reissue Application. Such is not the case with Nemo.

Since Nemo was published less than one (1) year prior to the filing date of the original patent (Dec. 9, 1996) it cannot be relied on for rejecting the claims under 35 U.S.C. §102(b) either. So, the only section remaining under which Nemo can be an alleged prior art is 35 U.S.C. §102(a).

2. Nemo and Slavin are not necessarily prior art under 35 U.S.C. §102(a)

Moreover, Nemo and Slavin may not qualify as prior art, regardless of what section of 35 U.S.C. §102 is used, including 35 U.S.C. §102(a). The alleged priority dates of Nemo and Slavin are August 1996 and November 1996, respectively, pre-dating the filing date of the original patent (Dec. 9, 1996) by only four (4) and one (1) months, respectively. Hence, Applicants reserve the right to contest the use of Nemo and Slavin as prior art reference, including by antedating their invention relative to these references.

B. The Claimed Invention is Patentably Distinguishable from the Cited References: the Cited References do not Teach, Enable or Suggest the Claimed Invention

It is well established that for anticipation to be established two requirements must be met: 1) the reference must teach each and every element of the invention; and 2) the reference must provide an enabling disclosure of the invention. Merely mentioning any aspect of the invention, without more, is insufficient to meet the anticipation requirements.

To recap, in keeping with the purpose of the claimed invention as set forth in claims 1-7 and 9-61, the modulus n is a product of the k prime factors, where $k>2$ and where the k prime factors are random and distinct. Furthermore, as set forth in the claims, e.g., claim 2, d (the private key portion) is established as a function of the k prime numbers and e (the public key portion). As recited for example in claim 2, d is a multiplicative inverse of e(mod(lcm($p_1 -1$, $p_2 - 1 \ldots p_k$-1))); and, again, the k ($k>2$) distinct random prime numbers $p_1, p_2, \ldots p_k$ from which the modulus n is provided/computed are also used for establishing d.

For clarity, it is perhaps better to first point out how this is different from the teachings of each of the cited references. These differences can then be related back to the claims.

Starting with **Rivest**, one of the references relied on by the Examiner, it is noted that Rivest is in fact incorporated by reference into the original patent. Rivest provides background information on the RSA public key encryption and sets the starting point for the claimed invention. No doubt, Rivest teaches and enables two-prime RSA public key encryption ($n=p \cdot q$). However, although Rivest discloses that alternative embodiments may use *n* which is a product of three or more primes, it specifically also states (and teaching away from the present invention) that the primes need not be distinct (col. 13, lines 29-31). In further contrast to the claimed invention, Rivest also makes no mention of the fact that such primes are distinct and random. The mere mention of three or more prime numbers without more does not rise to the level of enabling disclosure that would allow someone to practice the claimed invention without undue experimentation. (Needless to say, no one in the RSA universe has produced a product embodying the multi-prime RSA technology until the original patent came to light.)

Although in col. 13, lines 29-34, Rivest mentions CRT (Chinese remainder theorem) and perhaps can be understood to suggest an approach using sub-tasks, Rivest does not mention performing such sub-tasks in parallel and indeed does not makes a claim of improved performance as a result of using CRT (See: Section 50 of the Office Action). Moreover, Fig. 3, on which the Examiner relies (in Section 58), shows an encoding device (12) having registers (20, 22, 12, 24, 26 and 30), a multiplier selector (28) and a modulo *n* multiplier (32). As shown and described, neither the encoding device nor any part thereof are an exponentiation device. Namely, Rivest does not teach or suggest one or more exponentiation devices.

Vanstone, the next reference the Examiner relied on, is no more relevant than the foregoing reference. Vanstone introduces two concepts that address the need for added security with a stronger modulus. The first concept is using 4 prime factors in RSA which are selected from the same database as 2-prime RSA (See: Vanstone's *Introduction* and *Using four-primes RSA*). The second concept is selecting a set of primes that meet a non-random criteria. With these two concepts Vanstone teaches away from the present invention. Vanstone does not cover instances where the number of primes is K=3 and K>4, and it merely teaches the extension of 2 prime factors to 4 prime factors for a greater modulus *n*. More importantly, Vanstone suggests using the same database of primes as was used in 2-prime RSA. Namely, randomly selecting a

number from an existing list or a database is not selecting a random number from the universe of prime numbers. What is more, the 4 prime factors of n are not random in that they are related in Vanstone through a relationship of the form $p_i=2^k f_i+a_k$ (See: S.A. Vanstone et al. p. 2118).

Incidentally, Vanstone teaches a variant RSA. Vanstone suggests selecting a random e (See: Vanstone's *Using four-primes RSA*). As appreciated by the encryption community, this approach does not contribute to expedited cryptography. The opposite is true because a random e can be as large as n and exponentiation with such e can be extremely slow.

Nemo, another one of the cited references, discloses three-prime RSA (i.e., building n from three primes) and provides a processing time comparison between two-prime and three-prime RSA encryption methods. Ignoring for a moment the fact that Nemo may not qualify as a prior art, Nemo does not teach or suggest each and every element of the invention nor does it enable the invention as described above. Specifically, Nemo does not teach or suggest using at least three prime numbers $p_1, p_2, \ldots p_k$ from which the modulus n is provided/computed that are both distinct and random (See: Nemo's Section 4.3). Of course, Nemo fails also to address such features as the parallel processing of sub-tasks and the structural elements of the encryption system (e.g., with exponentiators for parallel processing).

Nemo also does not enable practice of the invention, including the need to use the k distinct and random prime numbers for establishing d in the manner as described above. Merely stating that, as a minor benefit, n can be build from three primes and that the likelihood of a random 256-bit number being prime is greater than the likelihood of a random 384-bit number being prime is not sufficient to enable the present invention (See: Nemo Section 4.3). In order to both teach and enable the present invention all the elements as described above must be found in Nemo. But, as just pointed, Nemo's disclosure is deficient with regard to both criteria for anticipation.

Slavin, the third reference the Examiner relied on for rejecting the claims, discloses a scheme for monitoring compliance of a public key encoding key using differential security levels (See: title, abstract, and claims 1-13 at col. 13-14). In fact, unlike the present invention as recited in claines 1-7 and 9-61, Slavin is not about multi-prime RSA, but rather is about using differential security levels (where unbalanced-RSA happens to be one possible encryption method). Slavin teaches away from using multi-prime in that it recommends against general use

of multi-prime (col. 7 lines 6-8 and 49-53). In stating that for a given n smaller primes result in less security Slavin fails to appreciate the value of multi-primes in RSA for general use.

Slavin discloses, in col. 7 line 37, preferably "using four [4] randomly selected prime numbers p_1, q_1, p_2, q_2, all of different values." However, when read in the context of Slavin's entire disclosure, including Slavin's claims, this assertion has a more limited meaning. For example, in col. 3, lines 17-26, Slavin discloses using no more than 4 primes unlike the present invention in which $k>2$ can be also $k>4$. Besides, in col. 4, lines 8-13, Slavin discloses that all of the recipient public keys are generated using typically different prime factors that are unlikely to have been selected by another user. In claim 6, Slavin recites "selecting a plurality of prime numbers" without mention of discrete or random. Namely, Slavin does not consider the prime numbers being random and different (discrete) a necessary element, or else Slavin would have recited them this way. In claims 1 and 11, Slavin doesn't even address the plurality of primes. Furthermore, in col. 4, lines 38-60, Slavin discloses that, preferably, the product of the pair of primes p_2, q_2, is substantially larger than either one of the primes p_1, q1 (lines 45-51); and that p_1, q_1 are two limited-size factors (lines 38-43).

As mentioned before, it is well settled that for anticipation the reference must teach each and every element of the claimed invention and must be enabling. As shown, the mere mention of four random different primes does not rise to the level of enabling disclosure. This assertion is supported in more than one way by Slavin's disclosure as outlines above. And, unlike the claimed invention wherein it is essential to have k random distinct prime numbers, the fact that Slavin does require the prime factors to be discrete and random, and in fact places size restrictions on them, teaches away from making this feature an essential element. As such, Slavin's disclosure is non enabling in that it does not avoid undue experimentation, considering the universe of prime numbers, in order to find that only discrete random primes can be employed to exercise the invention and produce the benefits associated with it.

In addition, and no less important, is the fact that Slavin discloses encapsulating the encoded message with the registered public key $\{n,e,g\}$ before it sent by the sender (See, e.g., col. 7, line 58 to col. 8 line 9, col. 12, lines 9-13). Namely, after the message is encoded with the recipient's public key (n,e), but before it is sent by the sender it is encapsulated. Contrast this with the claimed invention according to which the sender does not modify the encoded message

(be is ciphertext or signed message; See, e.g., explanation of the invention in the previous Section XIV).

Slavin also does not teach or suggest, and does not enable, creating the signed message as a function of the private key (*d,n*) as recited in claim 9. As well, Slavin does not teach the coefficients or suggest the manner in which such coefficients are used in creating the ciphertext as recited in claim 7. Finally, although this is not an exhaustive comparison, from these examples one could easily understand that the claimed invention is patentably distinguishable from Slavin's teachings. Again, the analysis of Slavin is presented herein notwithstanding the fact that Applicants reserve their right to dispute the use of Slavin as prior art in the first place.

Itakura, the next cited reference the Examiner relied on, discloses a scheme for accountable-group multi-signatures as an extension of RSA public key encryption. Namely, Itakura discloses a signature system rather than an encryption system. As shown in Figs. 2 and 3, the conventional cryptographic key is signed by a verifier and further signed by an approver in a scheme somewhat similar to a certificate authority approval. In any event, although in Fig. 1, Itakura shows a random number key generator it also states that of the three prime numbers it uses two are large and one is small (See, e.g., abstract). Indeed, Itakura discloses that there are restrictions placed on the position numbers, r_i, and shows how to apply such restrictions and find an optimal combination of keys *p, q, & r* (See, page 5, Sections 3.2 & 3.3; e.g.,"Therefore, r should be as small as possible"). In every respect, Itakura does not disclose three more prime numbers that must be random and distinct. Contrast this with the present invention in which k random distinct prime numbers constitute an essential element. Moreover, the r_i keys are numbers assigned in order of (organization) hierarchy and are public not private.

In further contrast to the claimed invention, Itakura modifies the encoded message (by the accountable-group signatures) before sending it. Although Itakura discloses generating a signed message using the private key *d*, it does not provide an enabling disclosure for creating a ciphertext using the public key *e* with multi-primes (k>2). Furthermore, Itakura does not teach using coefficients $a_e,\ldots a_0$ in creating the ciphertext message in the manner as recited for example in claim 7. As before, this is not an exhaustive comparison but it highlights the fact that the claimed invention is patentably distinguishable from Itakura.

The other references which were cited but not relied on are deemed no more relevant than the foregoing references (Section 71 of the Office Action). Having said all that, and having

shown how the invention is patentably distinguishable over the cited references, it is respectfully submitted that the cited references do not support the claim rejections because they do not teach, suggest or enable the claimed invention.

Then, in further traversing the claim rejections, select comments made by the Examiner in Sections 32-69 of the Office Action are hereafter addressed. It is noted that in Sections 61-69, the Examiner did not treat the claims individually, but rather made comments relating to the specific references, Vanstone, Nemo,Slavin and Itakura, where each of these comments swept at once over the entire group of claims 1-7 and 9-61. Therefore, Applicants primarily rely on the explanation above which more specifically shows why the cited references neither teach nor suggest or enable the claimed invention as recited in claims 1-7 and 9-61.

Secondarily, as to claim 1 the Examiner relies on Rivest and suggests that to apply CRT (Chinese Remainder Theorem) the primes must be relatively primed in pairs, implying their distinctness (Section 33 of the Office Action). However, the Examiner imports this assertion into Rivest in order to attribute the distinct and random character of the primes to Rivest. As a matter of 102 rejection practice this is not allowed in order to provide for the deficiency in Rivest. Besides, the claimed invention is not restricted to CRT as a means for combining the results of the subtasks, when such subtasks are used. Further as to claim 1, the discussion above illustrates how this claim distinguishes over the cited references (Sections, 61-69 of the office Action). Accordingly, it is respectfully submitted that claim 1 is allowable over the cited references.

Noting also the Examiner's comments as to claim 2, Rivest does not disclose nor enable establishing *d* as a function of *n*, *e* and the *k* random and distinct primes. Moreover, as claim 2 includes all the elements of allowable claim 1 it is also allowable over the cited references (Sections 34 and 61-69 of the Office Action).

As to claims 3-6 and 11-12, even if Rivest mentions terminal 1 and terminal 2 it does not meet all the elements of such claims (as outlined above with respect to claims 1, 2, et seq.) The remaining references are deficient as well in view of the explanation above (Sections 35-38, 42-44 and 61-69 of the Office Action).

As to claim 7, Rivest likewise fails to disclose or enable using the *k* random and distinct primes. For the reasons as described above, this is true even if Rivest mentions the coefficients $a_e, \ldots a_0$ (Sections 39-40 and 61-69 of the Office Action).

As to claims 14-61, the foregoing arguments apply with equal force and effect (Sections 45-69 of the Office Action). To recap some of the differences, as to claims 18 and 19, for example, Rivest does not disclose or enable establishing *d* as a function of *n*, *e* and the *k* random and distinct primes (Sections 48, 49). As to claims 20-23 and 50-55, solving the subtasks in accordance with the present invention is not limited to CRT alone and the invention is not claimed with such limitation (Sections 50, 59). This is true even if CRT can produce performance advantage when performed serially; and it is clear that performance of CRT is not inherently parallel as it can be serial as well. Moreover, the structural elements of the encryption system (as recited in claims 45 et seq) and the parallel processing of the sub-tasks is not found in the references (Sections 54-58). As to claims 24-33, Rivest does not disclose or enable the *k* random and distinct primes nor does it address the comparison between the respective computation cycles in two-prime and multi-prime encryption schemes (Sections 51, 52). As to claims 34-39, Rivest does not address or suggest using the *k* random and distinct primes and does not worry about backward compatibility (Section 53). And, as to claims 56-61, it would not be inherent in Rivest to generate the *k* random and distinct primes (Section 60). At the time of Rivest and Vanstone's papers, for example, there was no key development and there is no proof of that in either of them. In fact, they resorted to selecting the primes from a list or databases. The fact that the primes were pre-existing in the list, rather than developed, is an important distinction for the purpose of encryption security. Again, no matter how large the database is, selection from a subset of numbers is not synonymous with selection of a random number. Selection of *k* random numbers is characterized in that each of the numbers is equally likely to be selected.

Accordingly, Applicants respectfully submit that claims 1-7 and 9-61 are allowable over the cited references. Reconsideration and withdrawal of the claim rejections under 35 USC 102 are hereby respectfully solicited.

XVI. Double Patenting Rejection Over Co-pending Application

The Examiner provisionally rejected claims 9, 11, 12, 35 and 50-55 over claims in co-pending Application by the same inventors (09/328,726). The claims as now presented in this Reissue Application are distinguishable from claims 14-62 in the co-pending Application. Accordingly, Applicants believe that a Terminal Disclaimer is not warranted at this time.

Applicants respectfully request that this rejection be reconsidered and withdrawn or at the very least be withheld until issue of one of the Applications as a patent

XVII. Conclusion

A. Summary

Applicants appreciate the Examiner's review of this Reissue Application and respectfully request reconsideration and allowance of the pending claims 1-7 and 9-61 as now presented in view of the foregoing amendments and remarks. Applicants believe that all the objections and rejections have been overcome and that the Reissue Application is in condition for allowance.

B. Interview Requested

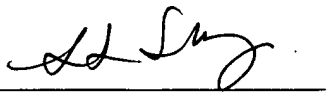
If any issues remain unresolved, the Examiner is kindly requested to contact the undersigned Applicants' attorney. Applicants appreciate the opportunity to discuss such issues with the Examiner in order to expedite the examination of this Reissue Application.

C. Fee Authorization:

If for any reason an insufficient fee has been paid, the Commissioner is hereby authorized to charge any deficiency in payment of required fees associated with this communication to Deposit Account **02-3964.**

Date: September 6, 2002

Respectfully submitted,



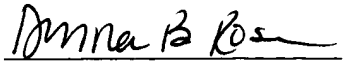
Leah Sherry,
Attorney for Applicant, Reg. No. 43,918

Oppenheimer Wolff & Donnelly LLP
Customer No. 25696
1400 Page Mill Road,
Palo Alto, CA 94304
Tel: (650) 320-4000

CERTIFICATE OF MAILING (37 CFR 1.8)

I hereby certify that this correspondence (along with all referenced and attached papers) is being deposited with the U.S. Postal Service in an envelop with sufficient postage as first class mail addressed to Box Reissue Patent Application, Assistant Commissioner for Patents, Washington, D.C. 20231, on

date: Sept. 10 2002



CONSENT OF ASSIGNEE TO REISSUE APPLICATION	Docket Number: 20206-014(PT-TA-410)

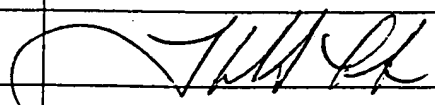
This is part of the application for a reissue patent based on the original patent identified below.

Name of Patentee(s):	COLLINS et al.		
Patent Number:	5,848,159	Patent Issued	December 8, 1998
Title of Invention	PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD		

As an authorized agent empowered to act on behalf of Compaq Computer Corporation, the assignee of the entire interest in the original patent, I hereby consent to the filing of the present application for reissue of the original patent.

☒ A certificate under 37 CFR(b) is attached.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application, any patent issued thereon, or any patent to which this declaration is directed.

Name of Assignee	Compaq Computer Corporation
Signature of Person Signing for Assignee	
Printed name and title of person signing for assignee	Theodore S. Park, Counsel

IN THE UNITED STATES PATENTS AND TRADEMARK OFFICE

Applicant: COLLINS et al. Attorney Docket No.: 20206-0014(PT-TA-410)

Patent No.: **5,848,159**

Issued: December 8, 1998

For: **"PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD"**

CERTIFICATE UNDER 37 CFR 3.73(b)

I. Compaq Computer Corporation, a Delaware corporation, certifies that it is the assignee of the entire right, title, and interest in the patent application identified above by virtue of a chain of title from the inventors of the patent application identified above, to the current assignee as shown below:

1. From: Thomas Collins, Dale Hopkins, Susan Langford and Michael Sabin
   To: Tandem Computers Incorporated

   The document was recorded in the Patent and Trademark Office on May 7, 1997 as Reel and Frame # 8542/0875.

2. From: Tandem Computers Incorporated
   To: Compaq Computer Corporation

   The document was recorded in the Patent and Trademark Office on October 12, 2000, a copy of which is attached.

II. The undersigned is empowered to sign this certificate on behalf of the assignee.

Date: 17 OCT 00

Theodore S. Park
Senior Counsel, Intellectual Property

Compaq Computer Corporation
P.O. Box 692000
Houston, TX 7707-2698

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
ASSISTANT SECRETARY AND COMMISSIONER
OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

JULY 15, 1997 97 JUL 22 AM 9:59

PTAS

TOWNSEND AND TOWNSEND AND CREW LLP
ROBERT J. BENNETT
TWO EMBARCADERO CENTER, 8TH FLOOR
SAN FRANCISCO, CA 94111-3834

100436861A

UNITED STATES PATENT AND TRADEMARK OFFICE
NOTICE OF RECORDATION OF ASSIGNMENT DOCUMENT

THE ENCLOSED DOCUMENT HAS BEEN RECORDED BY THE ASSIGNMENT DIVISION OF THE U.S. PATENT AND TRADEMARK OFFICE. A COMPLETE MICROFILM COPY IS AVAILABLE AT THE ASSIGNMENT SEARCH ROOM ON THE REEL AND FRAME NUMBER REFERENCED BELOW.

PLEASE REVIEW ALL INFORMATION CONTAINED ON THIS NOTICE. THE INFORMATION CONTAINED ON THIS RECORDATION NOTICE REFLECTS THE DATA PRESENT IN THE PATENT AND TRADEMARK ASSIGNMENT SYSTEM. IF YOU SHOULD FIND ANY ERRORS OR HAVE QUESTIONS CONCERNING THIS NOTICE, YOU MAY CONTACT THE EMPLOYEE WHOSE NAME APPEARS ON THIS NOTICE AT 703-308-9723. PLEASE SEND REQUEST FOR CORRECTION TO: U.S. PATENT AND TRADEMARK OFFICE, ASSIGNMENT DIVISION, BOX ASSIGNMENTS, NORTH TOWER BUILDING, SUITE 10C35, WASHINGTON, D.C. 20231.

RECORDATION DATE: 05/07/1997

REEL/FRAME: 8542/0875
NUMBER OF PAGES: 4

BRIEF: ASSIGNMENT OF ASSIGNOR'S INTEREST (SEE DOCUMENT FOR DETAILS).

ASSIGNOR:
COLLINS, THOMAS — DOC DATE: 04/29/1997

ASSIGNOR:
HOPKINS, DALE — DOC DATE: 04/29/1997

ASSIGNOR:
LANGFORD, SUSAN — DOC DATE: 04/30/1997

ASSIGNOR:
SABIN, MICHAEL — DOC DATE: 04/30/1997

ASSIGNEE:
TANDEM COMPUTERS INCORPORATED
10435 NORTH TANTAU AVENUE
CUPERTINO, CALIFORNIA 95014

SERIAL NUMBER: 08784453 — FILING DATE: 01/16/1997
PATENT NUMBER: — ISSUE DATE:

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
ASSISTANT SECRETARY AND COMMISSIONER
OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

DECEMBER 28, 2000

PTAS

101502720A

OPPENHEIMER WOLFF & DONNELLY LLP
LEAH SHERRY
1400 PAGE MILL RD.
PALO ALTO, CA 94304

UNITED STATES PATENT AND TRADEMARK OFFICE
NOTICE OF RECORDATION OF ASSIGNMENT DOCUMENT

THE ENCLOSED DOCUMENT HAS BEEN RECORDED BY THE ASSIGNMENT DIVISION OF THE U.S. PATENT AND TRADEMARK OFFICE. A COMPLETE MICROFILM COPY IS AVAILABLE AT THE ASSIGNMENT SEARCH ROOM ON THE REEL AND FRAME NUMBER REFERENCED BELOW.

PLEASE REVIEW ALL INFORMATION CONTAINED ON THIS NOTICE. THE INFORMATION CONTAINED ON THIS RECORDATION NOTICE REFLECTS THE DATA PRESENT IN THE PATENT AND TRADEMARK ASSIGNMENT SYSTEM. IF YOU SHOULD FIND ANY ERRORS OR HAVE QUESTIONS CONCERNING THIS NOTICE, YOU MAY CONTACT THE EMPLOYEE WHOSE NAME APPEARS ON THIS NOTICE AT 703-308-9723. PLEASE SEND REQUEST FOR CORRECTION TO: U.S. PATENT AND TRADEMARK OFFICE, ASSIGNMENT DIVISION, BOX ASSIGNMENTS, CG-4, 1213 JEFFERSON DAVIS HWY, SUITE 320, WASHINGTON, D.C. 20231.

RECORDATION DATE: 10/16/2000
REEL/FRAME: 011190/0457
NUMBER OF PAGES: 4

BRIEF: ARTICLES OF MERGER OF PATENT AND SUBSIDIARY CORPORATIONS

ASSIGNOR:
TANDEM COMPUTERS INCORPORATED
DOC DATE: 12/31/1998

ASSIGNEE:
COMPAQ COMPUTER CORPORATION
P.O. BOX 692000, 20555 SH 249
HOUSTON, TEXAS 77070-2698

SERIAL NUMBER: 08784453
FILING DATE: 01/16/1997
PATENT NUMBER: 5848159
ISSUE DATE: 12/08/1998

MARY BENTON, EXAMINER
ASSIGNMENT DIVISION
OFFICE OF PUBLIC RECORDS

UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Collins et al. Patent No. 5,848,159

Issued: December 8, 1998 By: LSB/jmp

Docket No. 20206-014(PT-TA-410) Express No. EL655031318US

For: **PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD**

The stamp of the U.S. Patent and Trademark Office hereon acknowledges receipt of the following:

1. Reissue Transmittal along with Fee Transmittal;
2. Petition to Wave Delay Period (37 CFR 1.183);
3. Specification and Claims for U.S. Patent No. 5,484,159;
4. Reissue Declaration by Inventors;
5. Offer to Surrender;
6. Certificate under 37 CFR 3.73(b);
7. Consent of Assignee to Reissue Patent;
8. Copy of Assignments;
9. Preliminary Amendment;
10. IDS Transmittal, 1449, and 13 cited references; and
11. Check No. 124516 for $2,664..00.